CPSC 536W: Homework 2

Due on Canvas by 11:59pm on 1st March 2024

Rules.

1. Please try to solve the problems yourself first. If you get stuck, you may consult any resources (books, internet, peers, office hours, etc.) for solutions. Provided you *acknowledge* these resources in detail, no marks will be deducted.
2. Please write legibly, work that is illegible will be marked as incorrect. Latex is strongly recommended for legibility. (I also recommend using `https://www.overleaf.com/` if you're new to Latex.)
3. All answers should be justified.
4. The total number of points for non-bonus questions is $T = 30$. Credit policy for the bonus questions: suppose you receive x points for the bonus questions and y points for the non-bonus questions, then the total number of points you receive for this homework is $\min(x + y, T)$.

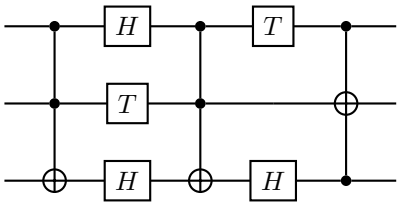
Homework

1. **Consolidation of lecture material.**

   (a) **Quantum circuits.** The following exercise is intended to explain the pictorial representation of quantum circuits by means of an example. Hopefully, the generalization of the example is obvious.
   The quantum circuit on 3 qubits (i.e, the "$a \in \mathbb{N}$" of the circuit is 3) defined by the sequence

   $$(\text{Toffoli}, (2,1,3)), (H,1), (T,2), (H,3), (\text{Toffoli}, (1,2,3)), (T,1), (H,3), (\text{Toffoli}, (3,1,2)), \tag{1}$$

   is pictorially representated as

   (1 point) Explain why $(\text{Toffoli}, (2,1,3))$ and $(\text{Toffoli}, (1,2,3))$ have the same pictorial representation but that their representations differ from that of $(\text{Toffoli}, (3,1,2))$. (Hint: look at the interpretation of the Toffoli gate defined in lecture 5 notes.)
   (1 point) Explain why in the column after the first Toffoli gate, the H, T, H gates are pictorially placed in the same column even though in the sequence eq. (1) H comes first, T second, and another H third. (Hint: look at the interpretation of the H and T gates defined in lecture 5 notes.)
   (1 point) Suppose the sequence of gates in eq. (1) is applied to $|000\rangle$ (that is, we sequentially multiply the unitary interpretations of these gates in order from left to right onto $|000\rangle$), what is the state at the end? Your answer should be in the form $\sum_{x \in \{0,1\}^3} \alpha_x |x\rangle$, where $\alpha_x \in \mathbb{C}$. (Hint: it's easier if you use Dirac notation throughout.)
   (The sequential product of the unitary interpretations of gates in a quantum circuit is known as the "unitary implemented by that quantum circuit".)

   (b) **Time complexity of Grover search in the context of kSAT.** Recall that in kSAT, the relevent query problem is to compute $\text{OR}_{2^l}(x)$ where $x \colon \{0,1\}^l \to \{0,1\}$ and l is the number of variables of the kSAT formula.
   (1 point) Suppose $l = 2$ and $x(u_1, u_2) = u_1 \wedge u_2$. Construct a quantum circuit with gates in qGATES which implements the quantum oracle of x (viewed as a 4 bit string), $O_x \in \mathbb{C}^{8 \times 8}$. (Hint: this question is worth 1 point, don't overthink it! It may be useful to identify $\mathbb{C}^8$ with $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. If you're interested in learning how O_x can be constructed given an *arbitrary* classical circuit computing $x \colon \{0,1\}^l \to \{0,1\}$, I encourage you to watch: Watrous' lecture.)

Recall that Grover's algorithm not only employs O_x but also the following unitary

$$G \coloneqq \mathbb{1}_{2^l} - 2|\psi\rangle\langle\psi| \in \mathbb{C}^{2^l \times 2^l}, \tag{2}$$

and $|\psi\rangle \coloneqq \frac{1}{\sqrt{2^l}} \sum_{u \in \{0,1\}^l} |u\rangle$.

(2 points) In the case that $l = 2$, show how to simulate the effect of G in eq. (2) using a quantum circuit (with gates in qGATES). That is, construct a quantum circuit on $a+2$ (for some $a \in \mathbb{N}$) qubits implementing a unitary $U \in \mathbb{C}^{2^a} \otimes \mathbb{C}^4$, and an $x \in \{0,1\}^a$, such that

$$U\,|x\rangle\,|v\rangle = |x\rangle\,G\,|v\rangle\,, \tag{3}$$

for all $|v\rangle \in \mathbb{C}^4$. (Recall that $|x\rangle\,|v\rangle$ means $|x\rangle \otimes |v\rangle$ and $|x\rangle\,G\,|v\rangle$ means $|x\rangle \otimes G\,|v\rangle$.)

(Note that the $|x\rangle$ part of the state U acts on does not change and serves as a catalyst (aka *ancilla*) to the simulation. Since the $|x\rangle$ part does not change, it can be reused later on for further simulations.)

(c) **Instantiating quantum queries to tilde bits.** Recall that the quantum algorithm for the collision problem first classically queries $x_1, \ldots, x_k$. Assuming these are distinct (else a collision is found), the algorithm then computes the following

$$\mathrm{OR}^{0,k}_{n-k}(\tilde{x}_{k+1}, \ldots, \tilde{x}_n), \tag{4}$$

where for $j \in \{k+1, \ldots n\}$,

$$\tilde{x}_j \coloneqq \begin{cases} 1 & \text{if } x_j \in \{x_1, \ldots, x_k\} \\ 0 & \text{if } x_j \notin \{x_1, \ldots, x_k\} \end{cases}. \tag{5}$$

This question is about how to instantiate the quantum oracle of $\tilde{x} \coloneqq \tilde{x}_{k+1} \ldots \tilde{x}_n$ with two calls of the quantum oracle O_x of x, when $x_1, \ldots, x_k$ are known.

Recall that $x \in \{0, 1, \ldots, n-1\}^n$ in the collision problem, so $O_x \in \mathbb{C}^{n^2 \times n^2}$ is defined by

$$O_x\,|i\rangle\,|j\rangle = |i\rangle\,|j + x_{i+1} \mod n\rangle\,, \tag{6}$$

for all $i, j \in \{0, 1, \ldots, n-1\}$.

(1 point) Show how to instantiate $O_x^\dagger$ using one call of O_x, that is, show the existence of unitaries $U_1, U_2 \in \mathbb{C}^{n^2 \times n^2}$ such that:

$$\forall x \in \{0, 1 \ldots, n-1\}^n, \quad O_x^\dagger = U_1 O_x U_2 \tag{7}$$

(Hints: (i) do not think of the left and right hand sides in terms of matrices, but in terms of their actions on the basis $\{|i\rangle\,|j\rangle \mid i, j \in \{0, 1, \ldots, n-1\}\}$, (ii) how does $O_x^\dagger$ act on this basis?)

Let $F\colon \{0, 1, \ldots, n-1\} \to \{0, 1\}$ be defined by $F(s) = \mathbb{1}[s \in \{x_1, \ldots, x_k\}]$. Let $U_F \in \mathbb{C}^{2n \times 2n}$ be the unitary corresponding to F as defined in the proof of Fact (*) in lecture 4 notes. Since we have classically queried $x_1, \ldots, x_k$, we can call U_F an arbitrary number of times without using any further queries to O_x.

(1 point) Fill in the expressions for the two *s in the following manipulations, where $i \in \{k, \ldots, n-1\}$ and $b \in \{0, 1\}$:

$$\begin{aligned} \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^2 \ni |i\rangle\,|0\rangle\,|b\rangle &\overset{O_x \otimes \mathbb{1}_2}{\mapsto} |i\rangle\,|x_{i+1} \mod n\rangle\,|b\rangle \\ &\overset{\mathbb{1}_n \otimes U_F}{\mapsto} * \\ &\overset{O_x^\dagger \otimes \mathbb{1}_2}{\mapsto} * \end{aligned} \tag{8}$$

(You should observe that the effect of the above manipulations is the same as applying the quantum oracle of $\tilde{x}$ with the $|0\rangle$ state in the middle serving as the ancilla.)

(d) **Lemma used in Simon's algorithm.**

(2 points) Prove the following:

Lemma 1. *Let $x \in \{0,1\}^k$ and $|x\rangle = |x_1\rangle \ldots |x_k\rangle$ be a k-qubit state. Let $H^{\otimes k} \coloneqq H \otimes \cdots \otimes H$ (k times), where H is the Hadamard gate. Then*

$$H^{\otimes k}\,|x\rangle = \frac{1}{\sqrt{2^k}} \sum_{y \in \{0,1\}^k} (-1)^{x \cdot y}\,|y\rangle\,, \tag{9}$$

where $x \cdot y \coloneqq \sum_{i=1}^k x_i y_i$.

2. **SWAP test.**

Let $n \in \mathbb{N}$. Let $|\psi\rangle \coloneqq \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$ and $|\phi\rangle \coloneqq \sum_{x\in\{0,1\}^n} \beta_x |x\rangle$ be two n-qubit quantum states, where $\forall x \in \{0,1\}^n, \alpha_x, \beta_x \in \mathbb{C}$.

Let cSWAP denote the unitary matrix acting on $\mathbb{C}^2 \otimes \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$ defined by

$$\text{cSWAP}\,|0\rangle\,|x\rangle\,|y\rangle = |0\rangle\,|x\rangle\,|y\rangle \quad \text{and} \quad \text{cSWAP}\,|1\rangle\,|x\rangle\,|y\rangle = |1\rangle\,|y\rangle\,|x\rangle\,, \tag{10}$$

for all $x, y \in \{0,1\}^n$.

(2 points) Compute the following state

$$(H \otimes \mathbb{1}_{2^n} \otimes \mathbb{1}_{2^n})(\text{cSWAP})(H \otimes \mathbb{1}_{2^n} \otimes \mathbb{1}_{2^n})\,|0\rangle\,|\psi\rangle\,|\phi\rangle\,, \tag{11}$$

using Dirac notation throughout.

(2 points) Suppose we make the computational basis measurement on the first register, that is, we make the measurement defined by

$$\Pi_0 \coloneqq |0\rangle\langle 0| \otimes \mathbb{1}_{2^n} \otimes \mathbb{1}_{2^n} \quad \text{and} \quad \Pi_1 \coloneqq |1\rangle\langle 1| \otimes \mathbb{1}_{2^n} \otimes \mathbb{1}_{2^n}\,. \tag{12}$$

Show that the probability of measuring 0 is

$$\frac{1 + |\,\langle\psi|\phi\rangle\,|^2}{2}. \tag{13}$$

(2 points) Suppose a stranger gives you k n-qubit states $|\psi_1\rangle, \ldots, |\psi_k\rangle$ with the promise that either

(a) For all $i \in [k]$,

$$|\psi_i\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\,, \tag{14}$$

or

(b) For all $i \in [k]$,

$$|\psi_i\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{x\in S} |x\rangle\,, \tag{15}$$

for some $S \subseteq \{0,1\}^n$ of size $|S| = 2^{n-1}$. (The stranger does not tell you what S is.)

The stranger also does not tell you which case you're in. Nonetheless, show that for all $k \geq 20$ there is a procedure involving the SWAP test that, in either case, can help you correctly decide the case you're in with probability $\geq 99/100$.

Remark 1. *The last part of the question is meant to illustrate that even quantum states with non-negative amplitudes (i.e., the α_xs are non-negative) behave very differently from probability distributions. In the probabilistic analogue of this problem, the first case would correspond to k samples each chosen uniformly randomly from $\{0,1\}^n$, and the second case would correspond to k samples each chosen uniformly randomly from some $S \subseteq \{0,1\}^n$ of size $|S| = 2^{n-1}$. If you don't know what S is, distinguishing between these cases with probability $\geq 99/100$ would require $k = \Omega(2^n)$.*

3. **Circuit size lower bounds on RAM and QRAM. (Or, why RAM and QRAM fall outside the Turing model.)**

For $l \in \mathbb{N}$, let $\text{RAM}_l \colon \{0,1\}^l \times \{0,1\}^{2^l} \to \{0,1\}$ be defined by $\text{RAM}_l(i,x) = x_i$. Let C_l be a classical circuit with $l + 2^l$ input bits and 1 output bit (as defined in lecture 5 notes) that computes RAM_l.

(2 points) Show that the circuit size (i.e., the number of gates) of C_l must be $\Omega(2^l)$.

For $l \in \mathbb{N}$, let $\text{QRAM}_l \in \mathbb{C}^{2^l} \otimes \mathbb{C}^{2^{2^l}} \otimes \mathbb{C}^2$ be the unitary matrix defined by

$$\text{QRAM}_l\,|i\rangle\,|x\rangle\,|b\rangle = |i\rangle\,|x\rangle\,|b \oplus x_{i+1}\rangle\,, \tag{16}$$

for all $i \in \{0,1\}^l$, $x \in \{0,1\}^{2^l}, b \in \{0,1\}$. Let Q_l be a quantum circuit on $l + 2^l + 1$ qubits (as defined in lecture 5 notes) that implements the unitary QRAM_l.

(2 points) Show that the circuit size (i.e., the number of gates) of Q_l must be $\Omega(2^l)$. (Hint: think about what you did for the first part.)

Remark 2. *(Q)RAM stands for (Quantum) Random Access Memory. The RAM assumption is effectively that the circuit of C_l can be described in a number of steps that is polynomial in l. The QRAM assumption is effectively that the circuit of Q_l can be described in a number of steps that is polynomial in l. As this question shows, these assumptions fall outside the Turing model. These assumptions are motivated by specialized hardware, called RAM and QRAM, that allow for extremely fast retrival of information. While the existence RAM is well-established, the existence of QRAM is controversial — see, e.g., [Jaques and Rattew, 23].*

In the collision problem, to implement the U_F (as defined in 1(c)) time-efficiently requires us to make the QRAM assumption. It is an interesting open question whether there exists a depth-d quantum query algorithm $\mathcal{A}$ that computes Collision_n *with bounded error* $1/3$ *such that*

(a) $d = O(n^{1/3})$

(b) for $i = 0, 1, \ldots, d$*, the unitary* U_i *defining* $\mathcal{A}$ *can be described as a quantum circuit in* τ_i *steps without making the QRAM assumption and* $\sum_{i=0}^{d} \tau_i \leq O(n^{1/3})$.

A reference along this line is [Chailloux, Naya-Plasencia, Schrottenloher, 17].

The same open question about removing QRAM is outstanding for many other quantum algorithms, e.g., the one we discussed for directed-STCON in hypercube. (To avoid possible confusion, note that the results we proved for query complexity are independent of the RAM/QRAM assumption and are unaffected by this discussion.)

4. **Directed-STCON in $1 \times n$ lattice.** Let $n \in \mathbb{N}$. Observe that each $x \in \{0,1\}^{3n+1}$ can be used to specify a subgraph of the $1 \times n$ lattice (see fig. 1) by indicating the presence or absence of its $3n+1$ edges. For example, $x_1 = 1$ means bottom left-most edge is present, $x_2 = 0$ means the bottom second-left-most edge is absent, etc.

   Define

$$L_{1,n} \colon \{0,1\}^{3n+1} \to \{0,1\} \tag{17}$$

   by $L_{1,n}(x) = 1$ if and only if there is a *directed* path from the *bottom-left vertex* to the *top-right vertex* in the subgraph of the $1 \times n$ lattice as specified by x, where the direction is from *left-to-right* and *down-to-up*.

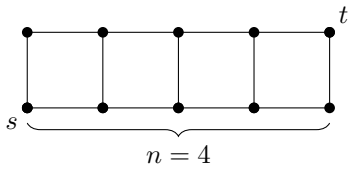


Figure 1: $1 \times (n = 4)$ lattice. s is the bottom-left vertex. t is the top-right vertex.

   (4 points) Show that $Q(L_{1,n}) = O(\sqrt{n})$.

   You may assume that when using Grover search to compute OR_k, the probability of error is zero.[1]

   (Hint: Grover search allows you to compute OR_k fast using $O(\sqrt{k})$ quantum queries, think about how computing various OR_ks on different subsets of bits of the input $x \in \{0,1\}^{3n+1}$ can be used to compute $L_{1,n}(x)$.)

   Remark 3. *There is an obvious generalization of this problem to the $k \times n$ lattice. Call the associated function $L_{k,n}$. It is known that $Q(L_{n,n}) = O(n^2)$ and, roughly speaking, $Q(L_{n,n}) = \Omega(n^{1.5})$. If you can improve the upper bound on $Q(L_{n,n})$ to $O(n^{2-\epsilon})$ for some $\epsilon > 0$, please let me know and I can help you prepare a paper for publication. Also see one of the bonus questions.*

5. **Directed-STCON in hypercube.** In class, we analyzed the directed-STCON in hypercube problem with one intermediate layer between Hamming weight zero and Hamming weight $n/2$.

   (6 points) Show how the analysis can be generalized to the case of *two* intermediate layers and derive an improved quantum query complexity upper bound for the problem.

   Your analysis should be at roughly the same level of detail as the lectured analysis. As in the previous question, you may assume that when using Grover search to compute OR_k, the probability of error is zero.

   Write your answer in the form $O^*(2^{cn})$ for some $c > 0$ written to 4 digits of accuracy. (Recall that $O^*(\cdot)$ means we ignore all polynomial factors in n.)

   (Hint: If you're stuck, you may consult [Ambainis et. al., 18]. However, you need to analyze the *two* intermediate layers case to receive any credit for this question.)

[1] In fact, the quantum query complexity of computing OR_k with exactly zero error is $\Theta(k)$, but using error suppression/Chernoff bound, it costs little to suppress the error to be tiny.

6. **Bonus questions.**

(2 points) General circuit construction for G. Show how to simulate the effect of the unitary G as defined in eq. (2) for *arbitrary* $l \in \mathbb{N}$. That is, construct a quantum circuit on $a+l$ (for some $a \in \mathbb{N}$) qubits with gates in qGATES implementing a unitary $U \in \mathbb{C}^{2^a} \otimes \mathbb{C}^{2^l}$, and an $x \in \{0,1\}^a$, such that

$$U\,|x\rangle\,|v\rangle = |x\rangle\,G\,|v\rangle\,, \tag{18}$$

for all $|v\rangle \in \mathbb{C}^{2^l}$.

(4 points) Circuit compilation. We use the symbol S to denote a quantum gate with unitary interpretation

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{19}$$

Prove or disprove the following statement.

For all unitaries $U \in \mathbb{C}^{2\times 2}$ and for all $\epsilon > 0$, there exists a quantum circuit on 1 qubit defined by a finite sequence of H (Hadamard) and S gates such that the unitary $V \in \mathbb{C}^{2\times 2}$ implemented by the quantum circuit satisfies

$$\|V - U\|_F \leq \epsilon, \tag{20}$$

where $\|\cdot\|_F$ denotes the Frobenius norm, i.e.,

$$\left\| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\|_F \coloneqq \sqrt{|a|^2 + |b|^2 + |c|^2 + |d|^2}. \tag{21}$$

(To receive any credit for this problem, you must prove/disprove from first principles. You may not invoke well-known theorems.)

Remark 4. *In the jargon, this question is asking whether the gate set $\{H, S\}$ is universal for single-qubit unitaries.*

(4 points) Directed STCON in $2 \times n$ lattice. Define $L_{2,n} \colon \{0,1\}^{5n+2} \to \{0,1\}$ in the obvious way for the function associated with directed-STCON in the $2 \times n$ lattice. That is, $L_{2,n}(x) = 1$ if and only if there is a directed path from the *bottom-left vertex* to the *top-right vertex* in the subgraph of the $2 \times n$ lattice as specified by x, where the direction is from *left-to-right* and *down-to-up*. (Note that there are $5n + 2$ edges in the $2 \times n$ lattice.)

Show that $Q(L_{2,n}) = O(\sqrt{n} \cdot \log^p(n))$, for some $p \geq 0$.

Again, you may assume that when using Grover search to compute OR_k, the probability of error is zero.

If you manage to do this question with $p = 0$, you will earn an additional 2 points (so 6 points).